

Guideline on Threats and Assets

Technical guidance on threats and assets in Article 13a

V1.1, March 2015





About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Dr. Marnix Dekker, Christoffer Karsberg

Contact

For contacting the authors please use resilience@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA worked with Giuseppe Colosimo and Alessio Baroni (Between, Italy) to develop the lists of threats and assets in this document. For the completion of this document ENISA has worked closely with a working group of experts from national regulatory authorities (NRAs) and ministries in the EU: the Article 13a Expert Group. Listing the organizations in the Article 13a expert group: PTS (SE), Agentschap Telecom (NL), FICORA (FI), Ofcom (UK), ANACOM (PT), ComReg (IE), EETT (GR), ADAE (GR), CFCS (DK), RTR (AT), ANCOM (RO), CRC (BG), Ministry of Economics Finance and Industry (FR), Bundesnetzagentur (DE), BIPT (BE), MINETUR (ES), MPO (CZ), CTO (CZ), CERT LT (LT), RU (SK), ILR (LU), AKOS (SI), MCA (MT), Ministry of Economic Development (IT), OCECPR (CY), Nkom (NO), ETSA (EE), RIA (EE), NMIAH (HU), ITSIRI (LV), UKE (PL), AKOS (SI), Teleoff (SK), OFCOM (CH), HAKOM (HR). We are grateful for their valuable input and comments.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2015

Reproduction is authorised provided the source is acknowledged.

Preface

The 2009 reform of the EU legislative framework for electronic communications (EU Directive 2009/140/EC) introduces Article 13a into the Framework directive (Directive 2002/21/EC as amended by Directive 2009/140/EC). The reform, was transposed by most EU Member States halfway 2011.

Article 13a concerns security and integrity of electronic communication networks and services. The first part of Article 13a requires that providers of networks and services manage security risks and take appropriate security measures to guarantee the security (paragraph 1) and integrity (paragraph 2) of these networks and services. The second part of Article 13a (paragraph 3) requires providers to report about significant security breaches and losses of integrity to competent national regulatory authorities, who should report about these security incidents to ENISA and the European Commission (EC) annually.

In 2010, ENISA, the European Commission (EC), Ministries and Telecommunication National Regulatory Authorities (NRAs), initiated a series of meetings (workshops, conference calls) to achieve an efficient and harmonised implementation of Article 13a across the EU. The Article 13a Expert Group now comprises experts from NRAs of most EU countries, and several EFTA and EU candidate countries. Meetings (telephonic or physical) are organized and chaired by technical experts from ENISA. The European Commission acts as an observer in these meetings.

The Article 13a Expert Group reached consensus on two non-binding technical guidelines for NRAs: the “Technical Guideline on Incident Reporting” and the “Technical Guideline on Security Measures”. This document complements the other two guides by providing a list of assets and a list of threats. This document provides a full list of threat types, the relation between threats and root cause categories (used in incident reporting), a full list of asset types, and it introduces asset groups and component layers.

The primary goal of this document is to improve pan-EU annual summary reporting. NRAs could also use this document for cross-checking risk assessments by providers, for supervising the security measures taken by providers, and for their national incident reporting frameworks.



Table of Contents

Preface	iii
1 Introduction	1
2 Article 13a	2
2.1 Paragraph 1 and 2 of Article 13a	2
2.2 Appropriate security measures	2
2.3 Security incidents	3
3 Risk assessment in Article 13a	4
4 Threats and causes	5
4.1 Threat types	5
4.2 Root cause categories	8
5 Assets and asset components	9
5.1 Asset types	10
5.2 Asset groups	13
5.3 Asset components	14
References	16
Related ENISA papers	16
EU Legislation	16
Relevant telecom architecture documents	16

1 Introduction

In this document, we provide guidance to National Regulatory Authorities (NRAs) about the risk assessment mentioned in paragraphs 1 and 2 of Article 13a of the Framework directive (Directive 2002/21/EC as amended by Directive 2009/140/EC).

This document is drafted by a working group comprising experts from NRAs and representatives of the EC, supported by technical experts from ENISA (see [Preface](#)): the [Article 13a Working Group](#).

Target audience

This document is addressed to national ministries and NRAs in European Member States, the authorities tasked with the implementation of Article 13a.

This document may be useful also for experts working in the EU's electronic communications sector and for experts working in the information security field.

Goal

This document is published by ENISA to provide NRA's with a vocabulary/glossary of terms to speak about threats and assets. This can directly be used in incident reporting (which is mandated by paragraph 3 of Article 13a) or used by NRAs to discuss with providers about their (internal) risk assessment (which is mandated by paragraph 1 and 2 of Article 13a).

Updates

ENISA updates this guideline periodically, when necessary and in agreement with the NRAs.

Structure of this document

In [Section 2](#) we introduce the relevant parts of Article 13a and some terminology used in this document. In [Section 3](#) we position this document vis-à-vis the supervision tasks of regulators. In [Section 4](#) we provide a list of detailed threat types, and we explain the five (broader) root causes categories. In [Section 5](#) we provide a list of asset types, which are commonly used in fixed and mobile telecommunications networks and we introduce a model off asset groups and component layers. In [Annex A](#) we provide a glossary of terms and acronyms commonly used to describe specific assets.

2 Article 13a

In this section we introduce Article 13a and the terminology used in this document.

2.1 Paragraph 1 and 2 of Article 13a

For the sake of reference, we reproduce the text of paragraphs 1 and 2 of Article 13a here.

“1. Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services. Having regard to the state of the art, these measures shall ensure a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks.

2. Member States shall ensure that undertakings providing public communications networks take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks. [...]”

In the interest of brevity, we use the following abbreviations:

- The term “provider” is used to refer to an “*undertaking providing public communications networks or publicly available electronic communications services*”.
- The term NRA is used to refer to competent “*national regulatory authority*” as mentioned in Article 13a, which could be a ministry, or a government agency, depending on the national situation.
- The term “networks and communication services” is used to refer to “*public communications networks or publicly available electronic communications services*” as mentioned in Article 13a. This includes mobile networks, public switched telephone networks, all-IP networks, mobile/fixed telephony and mobile/fixed internet access, etc.

2.2 Appropriate security measures

Paragraphs 1 and 2 of Article 13a contain two different requirements:

- Paragraph 1 requires providers to “*take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services*”, and to take measures “*to prevent and minimise the impact of security incidents on users and interconnected networks*”.
- Paragraph 2 requires providers to “*take all appropriate steps to guarantee integrity of their networks, and thus ensure the continuity of supply of services*”.

The use of the term integrity (of networks) in the article text may be confusing to some readers. We refer the reader to the definition in technical literature about networks and network interconnections¹, which defines integrity “*as the ability of the system to retain its specified attributes in terms of performance and functionality*”. Integrity of networks would be called availability or continuity in most information security literature.

We use the term ‘appropriate security measures’ to indicate the ‘appropriate technical and organisational measures’ and the ‘appropriate steps’ mentioned in the two paragraphs.

¹ Ward, K, 1995, ‘The Impact of Network Interconnection on Network Integrity’. British Telecommunications Engineering, 13:296–303.

The technical guideline on security measures provides an overview of different security measures that NRAs should take into account when assessing compliance of providers to these two paragraphs.

Both requirements use the term appropriate, and this means that providers should do a risk assessment. In this document we focus on the risk assessment.

2.3 Security incidents

Article 13a mentions ‘security incidents’, ‘security breaches’ and ‘integrity losses’:

- Paragraph 1 requires *“that measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks”*
- Paragraph 2 requires providers to *“take all appropriate steps to guarantee integrity of their networks, and thus ensure the continuity of supply of services”*.
- Paragraph 3 requires *“to notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services”*

We use one term for these incidents:

Security incident: A breach of security or a loss of integrity that could have an impact on the operation of electronic communication networks and services.

This definition is in line with the definition used in the document ‘Technical Guidelines for Incident Reporting’², which focusses on the process of incident reporting.

² Note that only a subset of these incidents have to be reported to ENISA and the EC, that is, those incidents that have had a significant impact on the continuity of services.

3 Risk assessment in Article 13a

Article 13a describes three main processes:

- 1) Provider assesses the risks, for its users and for the connected networks,
- 2) Provider takes “appropriate” security measures and
- 3) Provider reports about incidents to the NRA, should something go wrong.

The three processes are depicted in the diagram below.

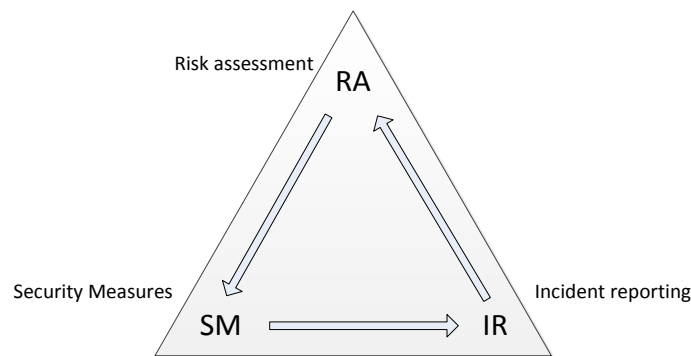


Figure 1 - The three security processes mandated by Article 13a.

Article 13a basically asks NRAs to supervise that these three processes are implemented adequately by the provider. Incidents could trigger an update of the risk assessment, and in this way lead to a change of security measures. So the processes feed into each other: Following a risk assessment a provider might want to take certain security measures. Vice versa, security measures which are in place, decrease certain risks. Incident reports provide feedback about the effectiveness of security measures, and they might lead to changes in the risk assessment.

This document is the third of three different guidelines, covering different aspects of this triangle:

- The Article 13a Technical Guideline on Incident Reporting is a guideline for NRAs about how to implement incident reporting
- The Article 13a Technical Guideline on Security Measures is a guideline for NRAs about how to supervise that providers take appropriate security measures,
- This guideline addresses the top of the triangle by providing a glossary or dictionary of the most common threat types and asset types. Our primary goal is to use this dictionary for incident reporting. Secondly, because threats and assets are the key components of risk assessments, this document may be used when making or evaluating risk assessments.

Remark about risk assessments and asset owners: *This guideline does not explain how providers can perform a risk assessment, nor does it rate the likelihood or impact of threats. Assessing risks is the responsibility of asset owners. Note that there are many different methods for performing risk assessments inside an organisation. Providers should use appropriate methods for performing risk assessments internally, depending on the type of organisation, the assets involved, the complexity of systems etc. Risk assessments need to be updated regularly, because risks change over time.*

Remark about using incident reporting to improve risk assessment: *Incident reporting (one of the obligations under Article 13a) could be used by NRAs to feed information about common threats and vulnerabilities back to the sector. For instance, NRAs could aggregate the received incident reports periodically and inform providers about common threats. In this way providers can improve their risk assessments, even before they experience a certain type of incident.*

4 Threats and causes

This section introduces a terminology (or dictionary) to speak about threats and causes.

We define a threat as follows³.

Threat: A threat is an event or a circumstance which could cause a security incident.

This definition is based on the definition of a security incident as defined in the incident reporting guideline (see also [Section 2](#)). The word “cause” is used to speak about a threat when it has already caused an incident (in the past).

The next section lists threat types. To explain what we mean with a threat *type* we give an example: A threat *type* would be “heavy wind”. The Gudrun storm (also called Erwin) of 2005, was a threat when it was forecasted to hit Denmark, Sweden and Estonia. When speaking about the security incident we call “heavy wind” (the Gudrun storm in this case) the cause of the incident.

4.1 Threat types

In this section we take a so-called “all-hazards” approach, i.e. all threats which could have an impact on the security of networks and services are in scope.

Note that this list of threat types is not exhaustive. We do not claim to make a taxonomy of threats here. We have not used a specific order for these threats, but grouped them according to similarities. For example we grouped natural phenomena together.

4.1.1 Heavy snow and ice

Heavy snowfall or ice can impact physical infrastructure, such as overland cables, base stations, overland power supply lines, et cetera.

4.1.2 Heavy wind

Heavy wind can impact physical infrastructure, such as overland cables, base stations, overland power supply lines, et cetera.

Note that in some cases incidents are caused by “bad weather”, i.e. a combination of “heavy wind” and “flood”.

4.1.3 Flood

Floods can impact physical infrastructure, such as server rooms, collocation sites, et cetera.

4.1.4 Earthquake

Earthquakes can impact physical infrastructure, such as power supply lines, underground and overland cables, sites, et cetera.

4.1.5 Wildfire

Wildfire can impact physical infrastructure, such as overland cables, overland power supply lines, collocation sites, et cetera.

³ This definition is similar to the definition in ISO27K5, which defines a threat as the cause of an incident.

4.1.6 Fire

Fire⁴ can damage physical infrastructure, such as cables, routers, server rooms, et cetera.

Note that this cause only covers accidental, unintentional instances of fire. For arson, see below.

Note that fire could also have an indirect impact, for example, when firefighters spray water or foam, or when they give orders to turn off power generators.

4.1.7 Arson

Arson (a fire started intentionally) could damage physical infrastructure, such as cables, servers, sites, street cabinets, et cetera.

Note there could also be an indirect impact, for example, when firefighters spray water or foam, or when they give orders to turn off power generators.

4.1.8 Electromagnetic interference

Electrical circuits and radio signals can be affected by electromagnetic interference. This kind of interference can be malicious (for example EMP guns), accidental (for example by a faulty transmitter) or part of a natural phenomenon (e.g. solar storms).

4.1.9 Denial of Service attack

A Denial of Service (DoS) attack aims to overload network or information systems with traffic. DoS attacks can have an impact on the continuity of networks or services.

4.1.10 Network traffic hijack

Attackers could change network routing or network addressing tables, which could have an impact on the security of the services, for example by altering BGP tables (BGP hijacks) or altering DNS zone files (DNS poisoning).

4.1.11 Malware and viruses

Malware and viruses can affect network and information systems, such as servers and applications. For example, there have been cases where malware was used to attack routers which impacted the network traffic of thousands of subscribers.

4.1.12 Advanced persistent threat

Advanced persistent threats, or APTs, are cyber attacks which are persistent (and stealthy, conspicuous), which target a range of different systems, often moving from one system to the other. APTs usually involve the manipulation of many different networks and information systems. For example an APT could target first a webserver, then the desktop computers of system administrators, and finally the firmware of core routers.

4.1.13 Hardware theft

Hardware theft could have an impact on networks and services, for example because thieves damage systems. Particularly multi-purpose IT equipment, or valuable items, such as large batteries, can be attractive for thieves.

⁴ Not to be confused with *wildfire* which is listed as separate cause.

4.1.14 Cable theft

Cable theft can have an impact on networks or services. For example, optical fiber cables could be cut when copper thieves dig up the cable searching for copper.

4.1.15 Cable cut

Cable cuts, for example by an excavation machine or ship anchorage, can have an impact on networks or services.

4.1.16 Power cut

Power cuts of the (public) powergrid, can have an impact on infrastructure which relies on power, for example basestations, sites, et cetera.

4.1.17 Power surge

Power surges, in the power supply of the main (public) powergrid, could have an impact on electronic devices connected to it.

4.1.18 Cooling outage

An outage of cooling systems can cause damage or malfunctioning of infrastructure.

4.1.19 Hardware failure

Hardware failures (when physical hardware breaks) could affect physical infrastructure such as servers, routers, base stations, et cetera, and in this way have an impact on networks and services.

4.1.20 Software bug

Software bugs could have an impact on ICT systems, such as routers, servers, databases, et cetera, and in this way impact networks or services. This type of threat also includes complex failures like network failures when several systems fail to connect or otherwise work together.

4.1.21 Design error

Design errors could have an impact on the security of networks and services. For example, an HLR handling 3G and 4G traffic could be designed wrong causing outages.

4.1.22 Faulty hardware change/update

A change or update of hardware, for example, for maintenance, replacement, or renewal, could go wrong and have a negative impact on networks or services.

4.1.23 Faulty software change/update

Software changes or updates, for example the installation of new software or software patches, could go wrong and have a negative impact on the networks or services. Note that this threat includes software like 'configuration files'.

4.1.24 Overload

Overload of traffic and usage could impact the networks and services.

4.1.25 Fuel exhaustion

Backup power generators can run out of fuel, which could have an impact on electronic devices.

Note this is typically a secondary cause for an incident, when the primary cause is power cut.

4.1.26 Policy or procedure flaw

A flaw in a policy or procedure, or the absence of a policy or a procedure, could have a negative impact on the networks or services.

4.1.27 Security shutdown

Security risks could force a provider to shutdown a service, for example to have the time to patch a software vulnerability.

4.2 Root cause categories

In this section we define 5 root cause categories⁵. Unlike the detailed threats/causes (defined in the previous section), root cause categories are broad categories describing the underlying problem.

Note that categorization of an incident in a specific root cause category often depends on the details and on the judgement of the NRA. For example, suppose a storm causes a power cut of several hours, which causes an outage because the fuel ran out in a backup power generators. Depending on the circumstances this may be categorized as a natural disaster (storm), human error (forgot to refill the fuel), or a system failure (refill procedure flawed).

4.2.1 Human errors

The category “human errors” includes the incidents caused by human errors during the operation of equipment or facilities, the use of tools, the execution of procedures, et cetera.

For example, suppose an employee of a provider made an error in following prescribed equipment maintenance procedures. The maintenance error caused an outage. In this case the incident would be categorized under ‘Human errors’.

4.2.2 System failures

The category “system failures” includes the incidents caused by failures of a system, for example hardware failures, software failures or errors in procedures or policies.

For example, if an HLR suddenly stops operating because of a software bug, which prevents all subscribers from connecting, then this incident would be categorized as ‘System failures’.

4.2.3 Natural phenomena

The category “natural phenomena” includes the incidents caused by severe weather, earthquakes, floods, wildfires, and so on.

For example, heavy winds cause a cable cut, causing outages, then the incident would be in the root cause category ‘natural phenomena’.

4.2.4 Malicious actions

The category “malicious actions” includes the incidents caused by a deliberate act by someone or some organisation.

⁵ The categories were derived from secondary legislation issued by FICORA and CESG UK.

For example, incidents which have a root cause like a fire started by employees as an act of sabotage, the poisoning of the provider's DNS systems by criminals, the hacking of the provider's computer systems, vandalism directed at street cabinets, and so on.

4.2.5 Third party failures

The category "third party failure" includes the incidents where the cause was not under direct control of the provider, but some third-party⁶.

For example, an outage caused by a cable cut caused by a mistake by the operator of an excavation machine used for a building a new road, would be categorized in the root cause category 'human error' and 'third-party failure'.

5 Assets and asset components

An asset is basically anything of value. Assets could be abstract assets (like processes or reputation), virtual assets (data for instance), physical assets (cables, a piece of equipment), human resources, money, et cetera.

In this guideline we focus on the following assets:

Scope: The assets in scope are those assets which support the provision of electronic communication networks and services.

This means that abstract assets like 'money' or 'reputation' are out of scope. Similarly, suppose a provider has an online store for selling smartphones and subscriptions. The shopping cart system is an asset, but it is out of scope of this guideline because it does not directly support the provisioning of network and communication services.

Remark on primary and secondary assets: *Often in literature there is a distinction between primary assets and secondary assets. For an electronic communications provider, the provisioning of services as well as the subscriber data are primary assets. But cables, routers, cooling systems, servers or HR processes are really secondary (or supporting) assets. Secondary assets are supporting the primary assets. As seen in the definition of scope, in this guideline the secondary/supporting assets are simply referred to as assets. In this guideline we do not use the word 'primary assets' and instead we refer more specifically to electronic communication networks and/or services.*

⁶ In the incident reporting this category is now used as a flag, in combination with another root cause category.

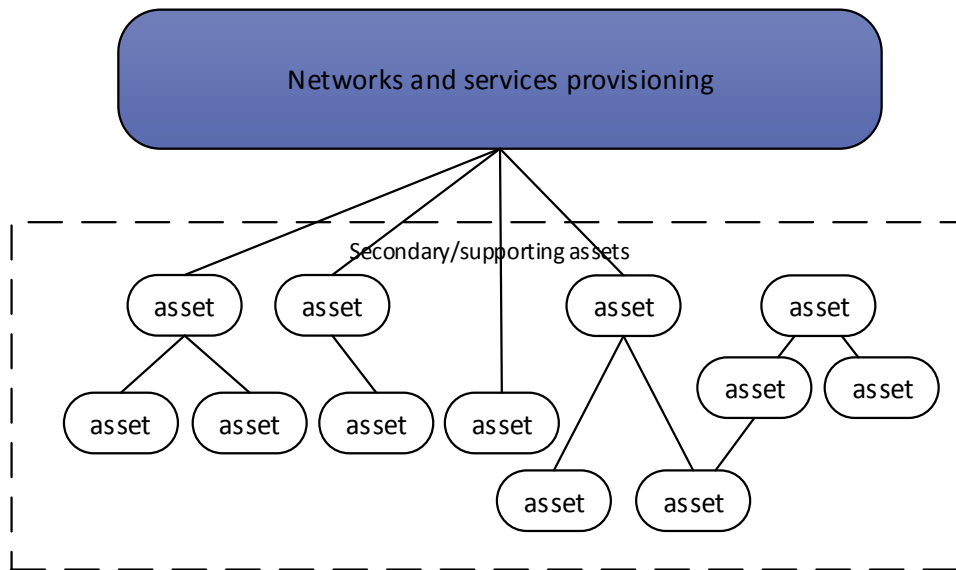


Figure 2: Assets in scope

Different providers use different assets, depending on the networks and services they provide, and depending on technical and architectural choices. Sometimes two similar assets can be used in a very different way by different providers. Sometimes the same asset is being called differently by different providers. This guideline introduces a vocabulary⁷ for speaking about the assets of providers. First of all this vocabulary is used for EU incident reporting from NRAs to ENISA and the EC. Secondly, because threats and assets are the main ingredients of a risk assessment, this allows NRAs and providers to evaluate and discuss the scope and outcome of risk assessments, and to discuss issues with specific assets, for example with providers, with other NRAs and ENISA.

5.1 Asset types

This section we provide a list of *asset types*. The term asset type is used to indicate a set of similar assets of providers. For example an asset type would be “mobile base stations and controllers”. A specific basestation (of a specific provider) is called an asset. Below, for the sake of clarity, we indicate for each asset type if it supports mobile or fixed networks, between square brackets.

Note that the list of asset types in this section is not exhaustive. Note also that a glossary of common terms, abbreviations and acronyms is included as an annex.

5.1.1 Subscriber equipment

[Mobile, Fixed]

Subscriber equipment, also known as user equipment (UE) or customer premise equipment (CPE), are systems at the subscriber’s premises, which are either fully or partially under control of the subscriber. This asset type is included here because in some settings the provider retains some control (and responsibility) over this equipment, for example, in the case of a managed PBX. See also [Section A.1](#).

⁷ It would perhaps be tempting to call this a taxonomy or a classification, but we would like to avoid these more formal words here. A taxonomy or a classification of assets would require a precise model of the provider’s assets, and it would be hard to create a model that fits all settings.

5.1.2 Switches and routers

[Mobile, Fixed]

Switches and routers are systems for switching and routing network traffic.

Examples: IP switches, routers, DSLAM, Hosted IP PBX, core (Tera-Giga) routers, Edge routers, SBC. See also [Section A.2](#).

5.1.3 Mobile user and location registers

[Mobile]

Mobile user and location registers, like HLRs and VLRs, are systems which keep records of subscribers, their subscriptions, their locations in mobile networks, etc.

Examples: HLR, AuC, HSS. See also [Section A.3](#).

5.1.4 Mobile base stations and controllers

[Mobile]

Mobile base stations and mobile basestation controllers are systems which provide subscribers access to the mobile networks of the providers.

Examples: BTS, BSC, NodeB and eNodeB, RNC, MME ANDSF, PCRF. See also [Section A.4](#).

5.1.5 PSTN switches

[Fixed]

PSTN switches are systems which switch traffic in legacy fixed voice networks (PSTN).

Examples: LE, TAX, AXE, Tandem Exchange. See also [Section A.5](#).

5.1.6 Mobile switches

[Mobile]

Mobile switches are systems used for switching in mobile networks.

Examples: MSC, VLR, SGSN, GGSN, PGW, SGW, ePGW. For more details see [Section A.6](#).

5.1.7 Transmission nodes

[Mobile, Fixed]

Transmission nodes are systems which perform data transport in optical networks.

Examples: SDH, WDM, DWDM. For more details see [Section A.7](#).

5.1.8 Addressing servers

[Mobile, Fixed]

Addressing services are used for look-up and addressing, like IP address allocation, domain name services, etc.

Examples: DHCP, DNS. For more details see [Section A.9](#).

5.1.9 Interconnection points

[Mobile, Fixed]

Interconnection points are used for exchanging traffic between the provider's network and networks of other providers.

Examples: IXPs, POP. For more details see [Section A.10](#).

5.1.10 Submarine cables

[Mobile, Fixed]

Submarine cables are cables and optical fibres rolled out on the seabed between two points on land, to carry telecommunication signals across stretches of ocean. A landing point is the location where a submarine or other underwater cable makes landfall.

5.1.11 Underground cables

[Mobile, Fixed]

Underground cables are underground physical network connections between active equipment (switches, routers, et cetera).

Examples: twisted copper pair, optical fibre, optical cable aggregation, cable aggregation. See also [Section A.11](#).

5.1.12 Over-the-air cables

[Mobile, Fixed]

Over-the-air cables are physical network connections between active equipment (switches, routers, et cetera).

5.1.13 Mobile messaging centre

[Mobile]

Mobile messaging centres are the assets providing messaging services in mobile networks.

Examples: SMS-C, MMS-C. See also [Section A.14](#).

5.1.14 Billing and mediation systems

[Mobile, Fixed]

Billing and mediation systems are the assets which performing billing in fixed and mobile networks. Mediation is the term used for converting usage and consumption data (length of calls, amount of data transferred) into billing and payment information.

5.1.1 Power supplies

[Mobile, Fixed]

Power supplies are the assets providing electrical energy to active equipment. Note this does not include the backup power supply.

Examples: Transformers, power lines, power connectors to the main grid, solar cells, etc.

5.1.2 Backup power supplies

[Mobile, Fixed]

Backup power supplies are the assets which ensure power backup functionality in case of power cut.

Examples: Diesel generators, batteries. See also [Section A.13](#).

5.1.3 Cooling systems

[Mobile, Fixed]

Cooling systems are the assets providing cooling or ventilation to network and information systems.

5.1.4 Street cabinets

[Fixed]

Street cabinets are assets which aggregate fixed connections. A street cabinet can hold passive and active network equipment, for copper, fibre or a combination of copper-fibre connections) and is typically located in the 'street' where it concentrates/aggregates local loop cables from subscribers.

5.1.5 Buildings and physical security systems

[Mobile, Fixed]

Buildings and physical security systems are the assets used by providers to protect other assets from physical and environmental threats.

Examples: Sites, data centers, fences, walls, doors, locks, et cetera.

5.1.6 Logical security systems

[Mobile, Fixed]

Systems providing logical protection of provider's network perimeter, including authentication, and authorization, encryption, and supporting services (e.g. directory information -LDAP).

Examples: firewalls, IDS/IPS, VPN servers, Radius, AAA systems, and LDAP. See also [Section A.15](#).

5.1.7 Operational support systems

[Mobile, Fixed]

ICT systems which support the operation of telecommunication networks. The term typically refers to systems managing the network and supporting processes such as maintaining a network inventory, configuring network components, managing faults, etc.

5.1.8 Intelligent network devices

[Fixed]

Intelligent network devices, typically in an SS7 architecture, provide additional services to the network assets allowing telecom operators to provide value-added services in addition to the standard communication services (e.g. number portability, green numbers, et cetera).

Examples: STP, SCP, SS7. See also [Section A.14](#).

5.2 Asset groups

Assets play a different role depending on their role and location in the provider's network. For example, a cable connecting two providers plays a very different role than a cable between a base station and a base station controller.

For the sake of clarity we group assets in 4 groups, depending on where the asset is located in the provider's network:

- Peering points – Assets in the group “Peering points” support the communications between the subscribers of one provider and the subscribers of another provider. For example, an IXP or a submarine cable, connecting several providers would be in this group.
- Core network – Assets in the group “Core network” support the bulk of the communications of the subscribers. For example, a backbone connecting two major cities in a country, or a central site would be in this group.
- Area network - Assets in the group “Area network” support a large part of the communications of the subscribers. For example, the cables between different parts of a large city or a regional site would be in this group.
- Access network – Assets in the group “Access network” support access of individual subscribers to the networks and communication services of the provider. For example, basestations or fiber-to-the-home infrastructure would be in this group.

The different asset groups are depicted below.

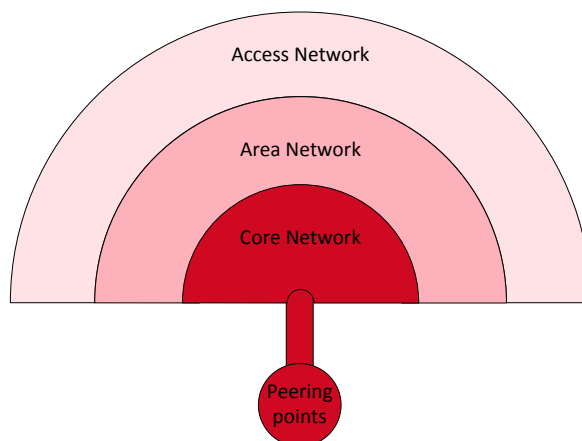


Figure 3: Assets are grouped in 4 main groups

Note that not all providers have assets in all groups. For example, some providers may just offer access network infrastructure, for others operators to use when offering services.

5.3 Asset components

For some assets, especially complex ICT assets, it can be useful to split them in several components.

For example, the components of a mobile basestations include the basestation’s operating system, the transceiver baseband unit, power amplifiers, power supply, its antenna’s, batteries and connection to the power grid.

For the sake of clarity we group these components in three different layers .

- Supplies layer – The Supplies layer consists of components such as power supply from the grid, or fuel supply from energy firms.
- Hardware layer –The hardware layer consists of hardware components.
- Software layer – The software layer consists of software components.

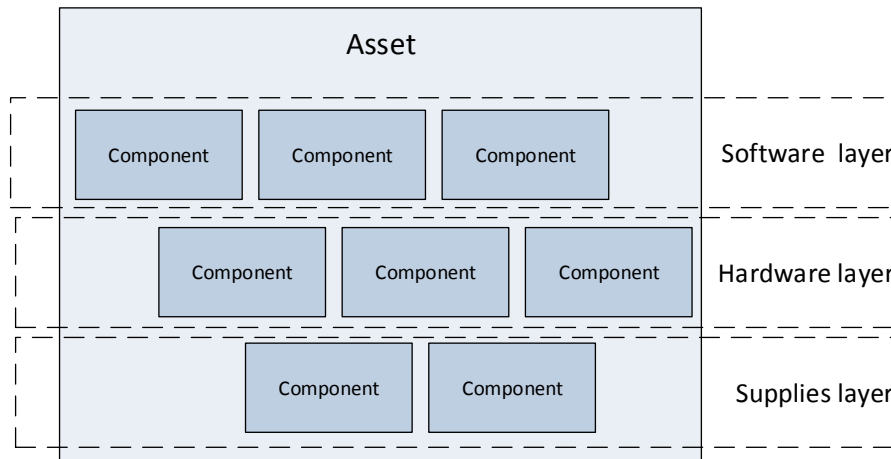


Figure 4: Assets consist of components at three different layers.

Note that not all assets have components in all layers. For example, a basic diesel generator, which has to be started manually, does not have components at the logical layer. A solar-cell powered base station does not have components at the supplies layer.

References

As references, we provide reference and a non-exhaustive list of common standards on risk assessment.

Related ENISA papers

- Annual reports of incidents are available at:
<https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports>
- Article 13a guidelines are available at: <https://resilience.enisa.europa.eu/article-13>
- ENISA's whitepaper on cyber incident reporting in the EU shows Article 13a and how it compares to some other security articles mandating incident reporting and security measures:
<http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu>
- For the interested reader, ENISA's 2009 paper on incident reporting shows an overview of the situation in the EU 3 years ago: <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/good-practice-guide-on-incident-reporting/good-practice-guide-on-incident-reporting-1>

EU Legislation

- Article 13a of the Framework directive of the EU legislative framework on electronic communications:
http://ec.europa.eu/information_society/policy/ecomm/doc/140framework.pdf
- The electronic communications regulatory framework (incorporating the telecom reform):
http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf
- An overview of the main elements of the 2009 reform:
http://ec.europa.eu/information_society/policy/ecomm/tomorrow/reform/index_en.htm
- The EU's cyber security strategy was adopted in 2013. The strategy contains a proposal for a directive on Network and Information Security. Article 14 of the proposed directive is basically an extension of Article 13a to other critical sectors.

Relevant telecom architecture documents

- Telecommunications Network and Service Architecture. Principles, Concepts and Architectures.
http://www.efort.com/media_pdf/ARCHITECTURES_EFORT_ENG.pdf
- Telecommunication Services Engineering: Definitions, Architectures and Tools.
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.19.1091&rep=rep1&type=pdf>
- Collaborative Procedures for Mobile Network Infrastructure Architectures. A Concept to Share Sensitive Information Between Competitors to Improve Situational Awareness and Protection. ASMONIA
http://www.asmonia.de/deliverables/D1.2_CollaborativeProceduresForMobileNetworkInfrastructureArchitectures.pdf
- Threat and Risk Analysis for Mobile Communication Networks and Mobile Terminals. ASMONIA

http://www.asmonia.de/deliverables/D5.1_II_ThreatAndRiskAnalysisMobileCommunicationNetworksAndTerminals.pdf

- The Internet and the Public Switched Telephone Network. Disparities, Differences, and Distinctions.

<http://www.internetsociety.org/sites/default/files/The%20Internet%20and%20the%20Public%20Switched%20Telephone%20Network.pdf>

- X.25 Architecture

[X.25 - Wikipedia, the free encyclopedia](#)

- X.25 Network Communications Overview

<http://publib.boulder.ibm.com/infocenter/aix/v6r1/index.jsp?topic=%2Fcom.ibm.aix.aixlink25%2Fdoc%2Fx25usrgd%2Foverv.htm>

Annex A: Glossary of terms for assets

In this annex we provide a glossary for terms providers may be using to refer to some of their assets.

A.1 Subscriber equipment

A.1.1 PBX

A private branch exchange (PBX) phone system is a system for handling call routing or switching, at the subscriber's location. Providers often offer PBX's as hosted services, and in these settings they manage the PBX equipment and software. Hosted IP PBX services can be delivered over the Internet (hosted IP PBX via Internet telephony, or VoIP). Traditional PBXs work via the PSTN public switched telephone network.

A.1.2 RG

Residential gateways (RG) are devices connecting local networks (LAN) to the network offered by the provider. The term residential gateway is often used to indicate gateways with less functionality compared to corporate gateways.

A.1.3 VoIP gateways

VoIP (Voice over IP) gateways are devices converting PSTN switched telephony traffic into IP packet switch traffic (SIP). Recently PBXs (see above) are often implemented using VoIP, for cost efficiency.

A.2 IP switches and routers

A.2.1 Metro routers

Metro routers are systems for routing traffic in metropolitan area networks.

A.2.2 Feeder

A feeder or aggregation switch is a multilayer switch installed in the same principal centrals of metropolitan and regional area, and it has the function of collecting and aggregating traffic from client devices and the access network. A remote feeder is a multilayer switch with redundant connections to two different feeder multilayer switches.

A.2.3 Routers

Routers perform routing of Internet protocol (IP) traffic. Tera routers and Giga routers are terms for IP routers handling Terabits or Gigabits of IP traffic per second.

A.2.4 Edge routers

Edge routers, also called provider edge routers, are routers at the edge of the provider's IP network.

A.2.5 DSLAM

A digital subscriber line access multiplexer (DSLAM) is a network device used in the access network, that connects multiple digital subscriber line (DSL) interfaces to a high-speed digital communications channel using multiplexing techniques.

A.2.6 SBC

A Session Border Controller (SBC) is a device in Voice over Internet Protocol (VoIP) networks for controlling signalling and media streams for telephone calls and interactive media communications. The SBC enforces security, quality of service and admission control of VoIP sessions.

A.3 Mobile user and location registers

A.3.1 HLR

The Home Location Register (HLR) is a central component in mobile networks that contains details of each mobile phone subscriber that is authorized to use the GSM core network.

A.3.2 AUC

The Authentication Centre (AuC) is a component of mobile networks GSM home locator register (HLR). The AuC validates any SIM card attempting network connection when a phone has a live network signal.

A.3.3 HSS

The Home Subscriber Server (HSS) is a master user database in mobile networks and it contains the subscription-related information (subscriber profiles), performs authentication and authorization of the user, and can provide information about the subscriber's location and IP information.

A.4 Mobile base stations and controllers

A.4.1 BTS

A base transceiver station (BTS) is a piece of equipment of mobile networks in access layer that ensure wireless communication between user equipment (UE) and a network.

A.4.2 BSC

The base station controller (BSC) provides in the access layer of mobile networks the intelligence behind the BTSs. Typically a BSC has tens or even hundreds of BTSs under its control.

A.4.3 NodeB and eNodeB

Node B is a term used in UMTS mobile networks equivalent to the BTS description used in GSM; the Evolved NodeB (eNodeB) is an element for fourth generation technology LTE.

A.4.4 RNC

The Radio Network Controller (or RNC) is a governing element in the UMTS mobile access network (UTRAN) and is responsible for controlling the nodes BS that are connected to it. The RNC carries out radio resource management, some of the mobility management functions and is the point where encryption is done before user data is sent to and from the mobile.

A.4.5 MME

The MME (Mobile Management Entity) is the key control-node for the LTE mobile access network. It is responsible for idle mode UE tracking and paging procedure including retransmissions. MME interacts with HSS for user authentication, it interacts with eNodeB and SGW for SGW selection, tunnel control, paging handovers, etc.

A.4.6 ANDSF

An Access Network Discovery and Selection Function (ANDSF) is an entity within a mobile evolved packet core network (EPC/LTE), which helps an UE to discover non-3GPP access networks, such as Wi-Fi or WIMAX – that can be used for data communications in addition to 3GPP access networks (such as HSPA or LTE) and to provide the UE with rules policing the connection to these networks.

A.4.7 PCRF

A Policy and Charging Rules Function (PCRF) is a software node to determine policy rules in a multimedia network. PCRF plays a central role in next-generation (IP) networks. A PCRF is a subscriber and application-aware policy decision point which interacts with the PGW to enforce per-session or per-flow policies.

A.5 Fixed switching

A.5.1 LE

A Local exchange (LE) is a central system of switches and other equipment which establishes connections between individual telephones.

A.5.2 TAX

A TAX (Trunk Automatic Exchange) switches (non-IP) long-distance calls in public switched telephone networks (PSTN).

A.5.3 Tandem exchange

A tandem exchange switches calls between LEs in a metro networks and handles spill over traffic from direct routes.

A.6 Mobile switching

A.6.1 MSC

A Mobile Switching Centre (MSC) is the primary service delivery node for GSM/CDMA mobile network, responsible for routing voice calls and SMS messages as well as other services (such as conference calls, FAX and circuit switched data).

A.6.2 VLR

A Visitor Location Register (VLR) is a database of mobile network subscribers in the area the MSC (Mobile Switching Centre) serves. Each base station in the network is served by one VLR.

A.6.3 SGSN

A Serving GPRS Support Node (SGSN) in a mobile network is responsible for the delivery of data packets from and to the mobile stations within its geographical service area.

A.6.4 GGSN

A Gateway GPRS support Node (GGSN) is a key component in a GPRS mobile network. The GGSN is responsible for the connections between the GPRS network and the external packet switched networks, like the Internet and X.25 networks.

A.6.5 PGW

A public data network Gateway (PGW) connects user equipment (UE) to external IP networks.

A.6.6 SGW

The SGW (Service Gateway) routes and forwards data packets, while acting as an anchor for the user plane during inter-eNodeB handovers and as the anchor for mobility between LTE and other 3GPP technologies.

A.6.7 ePDG

An ePDG (Enhanced Packet Data Gateway) secures data transmission between user equipment connected to the EPC over untrusted non-3GPP access (e.g. WLAN).

A.7 Transmission nodes

A.7.1 SDH, ADM, ROADM, ODXC

Synchronous Digital Hierarchy (SDH) is a method of digital transmission where the data is packed in containers, allowing multiplexing and de-multiplexing. SDH is a way to transfer multiple digital bit streams over optical fibres. For example ADM (Add Drop Multiplexer) is a multiplexing function used in SDH/SONET optical technologies.

A.7.2 WDM and DWDM

Wavelength-division multiplexing (WDM) and Dense wavelength division multiplexing (DWDM) is a technology which multiplexes a number of optical carrier signals into a single optical fibre by using different wavelengths (i.e. colours) of laser light. This technique enables bidirectional communications over one strand of fibre, as well as multiplication of capacity.

A.8 Addressing servers

A.8.1 DHCP

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assigning an IP address to new nodes entering the network.

A.8.2 DNS

The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. The DNS service commonly is supplied through IT components (e.g. servers).

A.9 Interconnection points

A.9.1 IXPs

An Internet exchange point (IX or IXP) is a physical infrastructure through which Internet service providers (ISPs) exchange IP traffic between their networks.

A.9.2 PoP (IP transit)

A Point of Presence (PoP) is a physical site or an artificial demarcation between different communications entities. It can be seen as an access point to the telecommunication provider network.

A.10 Underground and over-the-air cables

A.10.1 Twisted (copper) pair

Twisted pair is the ordinary copper wire that connects the subscriber to the provider's network. Wires are twisted to prevent interference from the outside.

A.10.2 Coaxial cables

Coaxial cables are cables containing a single copper wire, surrounded by insulation and a grounded shield of braided copper wire.

A.10.3 Optical fibres

Optical fibres are used for transmitting information by modulating a light beam (through the fibre). Optical fibres are more suitable for long distances and they have a higher bandwidth than wire cables.

A.11 Mobile messaging centres

A.11.1 SMS-C

A short message service centre (SMS-C) is a network element in the mobile telephone network and its purpose is to store, forward, convert and deliver SMS (Short Message Service) messages.

A.11.1.1 MMS-C

A MMS centre (MMS-C) is a network element in the mobile telephone network and its purpose is to store, forward, convert and deliver MMS (Multimedia Messaging Services) messages.

A.12 Backup power

A.12.1 Diesel generator

A diesel generator provides emergency power supply, by using diesel fuel.

A.12.2 UPS

An uninterruptible power supply, also uninterruptible power source, UPS or battery/flywheel backup, is an electrical apparatus that provides emergency power when main power supply fails.

A.13 Intelligent network devices

A.13.1 STP

A Signal Transfer Point (STP) is a component of Intelligent Network (IN, fixed and mobile telephony) and it's a device that relays SS7 messages between signalling end-points (SEPs) and other signalling transfer points (STPs).

A.13.2 SCP

A Service Control Point (SCP) is a standard component of the IN Intelligent Network (fixed and mobile telephony) telephone system which is used to control the service. Standard SCPs in the telecom industry today are deployed using SS7, SIGTRAN or SIP technologies.

A.14 Logical security systems

A.14.1 Firewall

Firewall is a software or hardware-based network security system that controls the incoming and outgoing network traffic by analysing the data packets and determining whether they should be allowed through or not, based on applied rule set.

A.14.2 VPN

A Virtual Private Network (VPN) extends a private network across a public network, such as the Internet. VPN function could be provided by firewalls, servers and end-points (PCs tablets, smartphones et cetera).

A.14.3 AAA

AAA commonly stands for authentication, authorization and accounting or auditability. It refers to a security architecture for distributed systems in which the identity of users is first authenticated, then users are granted access, and finally a log is kept of their access (for the sake of accounting or auditing).

A.14.4 LDAP

The Lightweight Directory Access Protocol (LDAP) is a protocol for accessing and managing a directory of information about users and their access rights. LDAP is typically used for finding information about users quickly in directories with large numbers of users.

**ENISA**

European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece



PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu